Journal of Mathematical Research with Applications
Mar., 2015, Vol. 35, No. 2, pp. 130–136
DOI:10.3770/j.issn:2095-2651.2015.02.002
Http://jmre.dlut.edu.cn

The Transfer Ideal under the Action of the Dihedral Group D_{2p} in the Modular Case

Jizhu NAN, Lingli ZENG*, Kai ZHANG
School of Mathematical Sciences, Dalian University of Technology, Liaoning 116024*, P. R. China*

Abstract In this paper, we determine the structures of the transfer ideal and its radical ideal for the ring of polynomials $F_p[x,y]$ under the action of dihedral group D_{2p} in the modular case. We mainly use Transfer variety, p order elements, and Hilbert's Nullstellensatz Theorem.

Keywords invariant; transfer ideal; transfer variety; radical ideal

MR(2010) Subject Classification 13A50; 37C30; 13A15

1. Introduction

Let G be a finite group, F be a field, and $\varrho : G \hookrightarrow GL(n,F)$ be a faithful representation of G over F. Then, via ϱ, G acts on the vector space $V = F^n$. We denote by $F[V] = F[x_1,\ldots,x_n]$ the graded algebra of polynomial functions on V, which is defined to be the symmetric algebra on V^*, the dual of V, in n indeterminate elements $x_1,\ldots,x_n$. Then this action can induce an action of G on $F[V]$ (see [1]):

$$gf(v) = f(\varrho(g^{-1})v),\ \forall g\in G,\ f\in F[V],\ v\in V.$$

The ring of invariants denoted by $F[V]^G$, is the fixed subalgebra, i.e.,

$$F[V]^G = \{\ f\in F[V] \mid gf = f,\ \forall g\in G\}.$$

The transfer homomorphism is an important tool to calculate the ring of invariants $F[V]^G$, and it is defined by

$$\begin{aligned} Tr^G : F[V] &\to F[V]^G \\ f &\to \sum_{g\in G} gf. \end{aligned}$$

The image of the transfer homomorphism is an ideal of the ring of invariants $F[V]^G$, we call it transfer ideal $\mathrm{Im}(Tr^G)$.

In the non-modular case, i.e., the order of G and the characteristic of F satisfied: $\mathrm{Char}\, F \nmid |G|$, it is easy to verify that the transfer homomorphism is surjective, so the ring of invariants $F[V]^G$ can be completely described by transfer ideal. In the modular case, i.e., $\mathrm{Char}\, F \,||G|$, it

Received April 14, 2014; Accepted June 18, 2014
Supported by the National Natural Science Foundation of China (Grant No. 11371343).
* Corresponding author
E-mail address: jznan@163.com (Jizhu NAN); zengll929@163.com (Lingli ZENG)

is more complicated and harder than the first case. Although the transfer homomorphism is not surjective [2, Section 2], and $\mathrm{Im}(Tr^G) \subseteq F[V]^G$ is a proper ideal of $F[V]^G$, but it also can provide a lot of information for the ring of invariants $F[V]^G$. Hence, it is necessary to determine the structure of the transfer ideal.

Let $\varrho : G \hookrightarrow GL(n, F)$ be a faithful representation of a finite group over the field F. The transfer variety, denoted by $\Omega_G \subseteq V$, is defined by [3, Section 6.4]

$$\Omega_G = \{v \in V | Tr^G(f)(v) = 0, \ \forall f \in \mathrm{Tot}(F[V])\}.$$

Let p be an odd prime, $D_{2p} = \langle a, b | a^p = 1, b^2 = 1, ab = ba^{-1} \rangle$ be the dihedral group of order $2p$. Let $\varrho : D_{2p} \hookrightarrow GL(2, F_p)$ be a faithful representation of the group D_{2p} over the prime field F_p, afforded by the matrices

$$\varrho(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \varrho(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In this paper, firstly, we obtain the p order elements of the dihedral group D_{2p} and transfer variety. Secondly, we apply Hilbert's Nullstellensatz Theorem to describe structures of the transfer ideal and its radical ideal for the ring of polynomials $F_p[x, y]$ under the action of D_{2p} in the modular case.

2. Transfer ideal $\mathrm{Im}(Tr^{D_{2p}})$ of D_{2p}

First, we recall the computation of the ring of invariants $F_p[V]^{D_{2p}}$.

Let $\varrho : D_{2p} \hookrightarrow GL(2, F_p)$ be a faithful representation of the group D_{2p} over the prime field F_p, afforded by the matrices

$$\varrho(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \varrho(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $F_p[V] = F_p[x, y]$. Then

$$a \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -x + y \end{pmatrix}, \ b \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}.$$

So the orbits of x, y under the action of D_{2p} are

$$o[x] = \{x, -x\}, \ o[y] = \{y, y - x, \dots, y - (p-1)x\} = \{y, y + x, \dots, y + (p-1)x\}.$$

Then we have $y \notin \bigcup_{g \in D_{2p}} \mathrm{Span}\{gx\}$, so x, y are Dade's basis, and the top Chern classes

$$C_{\mathrm{top}}(x) = -x^2, \ C_{\mathrm{top}}(y) = y^p - yx^{p-1}$$

are a system of parameters. Furthermore,

$$|D_{2p}| = \deg(C_{\mathrm{top}}(x)) \cdot \deg(C_{\mathrm{top}}(y)) = 2p,$$

then

$$F_p[V]^{D_{2p}} = F_p[x^2, y^p - yx^{p-1}].$$

Lemma 2.1 *The elements of order p in D_{2p} are $a^i, i = 1, \ldots, (p-1)$.*

Proof Since the generators a, b in D_{2p} satisfy $ab = ba^{-1}$, the elements in D_{2p} can be written in the form of a^ib^j, $i = 1, \ldots, (p-1), j = 0, 1$. And the representation

$$\varrho(a^ib) = \begin{pmatrix} (-1)^j & 0 \\ i & 1 \end{pmatrix},$$

ϱ is faithful, when $j = 1$, the order of $\begin{pmatrix} -1 & 0 \\ i & 1 \end{pmatrix}$ is 2; when $j = 0$, the order of $\begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$ is p. Hence, the elements of order p in D_{2p} are a^i, $i = 1, \ldots, (p-1)$. □

Lemma 2.2 $V^a = V^{a^i}, i = 1, \ldots, (p-1)$, *where V^a denote the fix points in V under the action of $a \in D_{2p}$.*

Proof On the one hand, $\forall v \in V^a$, $a(v) = v$, we have $a^i(v) = a^{i-1}(a(v)) = a^{i-1}(v) = \cdots = a(v) = v$, i.e., $V^a \subseteq V^{a^i}$. On the other hand, every non-identity element in the group (a) is a generator of the group (a), since the order of the cyclic group (a) is prime p. Then there is a number k, such that $a = (a^i)^k$. If $a^i(v) = v$, then $a(v) = v$, i.e., $V^{a^i} \subseteq V^a$. □

Since $\mathrm{Im}(Tr^G)$ is an ideal of $F[V]^G$, $F[V]^G \subseteq F[V]$ is ring extension. According to the definition of transfer variety $\Omega_G = \{v \in V | Tr^G(f)(v) = 0, \forall f \in \mathrm{Tot}(F[V])\}$, we have

$$\Omega_G = \{v \in V | f(v) = 0, \forall f \in (\mathrm{Im}(Tr^G))^e\} = V((\mathrm{Im}(Tr^G))^e),$$

where $(\mathrm{Im}(Tr^G))^e$ denotes the extension ideal of $\mathrm{Im}(Tr^G)$ in $F[V]$.

Lemma 2.3 ([3, Corollary 6.4.6]) *Let $\varrho : G \hookrightarrow GL(n, F)$ be a faithful representation of a finite group over the field F of characteristic p. Then*

$$\Omega_G = \bigcup_{g \in G, |g| = p} V^g,$$

i.e., transfer variety is the union of the fixed-point sets of the elements in G of order p.

Let $V = \{\lambda_1 e_1 + \lambda_2 e_2 | \lambda_1, \lambda_2 \in F_p\}$ be the vector space over the prime field F_p of dimension 2. Then the group D_{2p} has a natural action on V.

Lemma 2.4 *The fixed-point set of element a is $V^a = \{\lambda e_2 | \lambda \in F_p\}$.*

Proof Let $\lambda_1 e_1 + \lambda_2 e_2 \in V$. Then

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} e_1 + e_2 & e_2 \end{pmatrix},$$

and

$$a(\lambda_1 e_1 + \lambda_2 e_2) = \lambda_1(e_1 + e_2) + \lambda_1 e_2 = \lambda_1 e_1 + (\lambda_1 + \lambda_2) e_2.$$

If $\lambda_1 e_1 + \lambda_2 e_2 \in V^a$, then we have

$$a(\lambda_1 e_1 + \lambda_2 e_2) = \lambda_1 e_1 + \lambda_2 e_2.$$

So $\lambda_1 = 0$, and $V^a = \{\lambda e_2 | \lambda \in F_p\}$. □

Proposition 2.5 *Let $\varrho : D_{2p} \hookrightarrow GL(2, F_p)$ be a faithful representation of the group D_{2p} over the prime field F_p, afforded by the matrices*

$$\varrho(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \varrho(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $\sqrt{(\mathrm{Im}(Tr^{D_{2p}}))^e} = (x)_{F_p[V]}$, where $(x)_{F_p[V]}$ is the ideal generated by x in $F_p[V]$.

Proof By Lemma 2.1, we know that if $g \in D_{2p}$ and $|g| = p$, then $g = a^i, i = 1, \dots, (p-1)$. By Lemmas 2.2 and 2.4, we see

$$V^{a^i} = V^a = \{\lambda e_2 | \lambda \in F_p\}.$$

Furthermore, by Lemma 2.3, we have

$$\Omega_{D_{2p}} = \bigcup_{g \in D_{2p}, |g| = p} V^g = \bigcup_{i=1}^{p-1} V^{a^i} = V^a = \{\lambda e_2 | \lambda \in F_p\}.$$

If $\overline{F}$ is the algebraic closure of F_p and $\overline{\Omega}_{D_{2p}}$ the transfer variety over $\overline{F}$, then

$$\overline{\Omega}_{D_{2p}} = \Omega_{D_{2p}} \otimes_{F_p} \overline{F} = V^a \otimes_{F_p} \overline{F}$$

is the variety defined by the set of linear forms $\{kx \otimes_{F_p} 1 \mid k \in F_p\}$, for $(x \otimes_{F_p} 1) \cdot (e_2 \otimes_{F_p} 1) = 0$ and $(x \otimes_{F_p} 1) \cdot (e_1 \otimes_{F_p} 1) = 1 \otimes_{F_p} 1 \neq 0$. Hence

$$\overline{\Omega}_{D_{2p}} = \{\overline{v} \in \overline{V} = \overline{F}^2 \mid kx \otimes_{F_p} 1(\overline{v}) = 0, k \in F_p\}.$$

Thus, we get

$$V((\mathrm{Im}(Tr^{D_{2p}}))^e) = \overline{\Omega}_{D_{2p}} = V((x)_{\overline{F}[\overline{V}]}) \quad \text{in} \quad \overline{F}[\overline{V}].$$

By Hilbert's Nullstellensatz Theorem, it follows that

$$\sqrt{(\mathrm{Im}(Tr^{D_{2p}}))^e} = I(V((\mathrm{Im}(Tr^{D_{2p}}))^e)) = I(V((x)_{\overline{F}[\overline{V}]})) = \sqrt{(x)_{\overline{F}[\overline{V}]}}$$

in $\overline{F}[\overline{V}]$, then limit the result on the field F_p by flat base change which is the similar method to the example 1 on the page 276 in [3], that $\sqrt{(\mathrm{Im}(Tr^{D_{2p}}))^e} = \sqrt{(x)_{F_p[V]}}$ in $F_p[V]$, since x is defined over F_p. Hence $\sqrt{(\mathrm{Im}(Tr^{D_{2p}}))^e} = (x)_{F_p[V]}$, by $(x)_{F_p[V]}$ is a prime ideal. □

Suppose $p_i = x_1^i + \cdots + x_n^i$ are the ith symmetric power sums of $x_1, \dots, x_n$, and $s_i = s_i(x_1, \dots, x_n)$ are the ith elementary symmetric polynomials of $x_1, \dots, x_n$.

Lemma 2.6 (Newton's Formulae)([1, Proposition 4.7]) *The symmetric power sums p_i and elementary symmetric polynomials s_i satisfy the following relations:*

$$s_1 = p_1,$$

$$2s_2 = p_1 s_1 - p_2,$$

$$\cdots$$

$$is_i = \sum_{k=1}^{i} (-1)^{k-1} p_k s_{i-k},$$

where we set $s_0 = 1$.

Lemma 2.7 *In the prime field* F_p, $s_i(1,\dots,p-1) = 0, i = 1,\dots,p-2$.

Proof We consider the polynomial $\prod_{k=1}^{p-1}(x-k)$ in $F_p[x]$ with roots of all non zero elements of F_p. Since all non zero elements of F_p satisfy the equation $k^{p-1} = 1$, we know that they are roots of polynomial $x^{p-1} - 1$ in $F_p[x]$, hence $\prod_{k=1}^{p-1}(x-k) = x^{p-1} - 1$, which means $s_i(1,\dots,p-1) = 0, i = 1,\dots,p-2$. □

Lemma 2.8 *In the prime field* F_p, $\sum_{k=1}^{p-1} k^i = 0, i = 1,\dots,p-2$.

Proof By the Newton's Formulae in the Lemma 2.6, we have

$$is_i = \sum_{k=1}^{i} (-1)^{k-1} p_k s_{i-k}.$$

i.e.,

$$(-1)^{i-1} p_i = \sum_{k=1}^{i-1} (-1)^{k-1} p_k s_{i-k} - is_i.$$

Put the elements of the field F_p into preceding equation and by the Lemma 2.7, we see that $(-1)^{i-1} p_i = 0$, hence $\sum_{k=1}^{p-1} k^i = 0, i = 1,\dots,p-2$. □

Lemma 2.9 (Fermat's Theorem) ([4, Theorem 71]) *If p is a prime, and $p \nmid a$, then* $a^{p-1} \equiv 1 \pmod{p}$.

Lemma 2.10 ([5, Theorems 1.4.12, 1.4.13]) *Let A, B be two rings, $\Phi : A \to B$ be a ring homomorphism, $a \subseteq A$ is an ideal of A, then (1)* $a \subseteq a^{ec}$*; (2)* $(\sqrt{a})^e \subseteq \sqrt{(a^e)}$.

Theorem 2.11 *Let $\varrho : D_{2p} \hookrightarrow GL(2, F_p)$ be a faithful representation of the group D_{2p} over the prime field F_p, afforded by the matrices*

$$\varrho(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \varrho(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $\sqrt{\mathrm{Im}(Tr^{D_{2p}})} = (x^2)_{F_p[V]^{D_{2p}}}$.

Proof On the one hand, we have

$$\sqrt{\mathrm{Im}(Tr^{D_{2p}})} \subseteq (\sqrt{\mathrm{Im}(Tr^{D_{2p}})})^{ec}$$

by Lemma 2.10 (1).

Since $(\sqrt{\mathrm{Im}(Tr^{D_{2p}})})^{ec} = (\sqrt{\mathrm{Im}(Tr^{D_{2p}})})^{e} \bigcap F_p[V]^{D_{2p}}$, we have

$$(\sqrt{\mathrm{Im}(Tr^{D_{2p}})})^{e} \bigcap F_p[V]^{D_{2p}} \subseteq \sqrt{(\mathrm{Im}(Tr^{D_{2p}}))^{e}} \bigcap F_p[V]^{D_{2p}}$$

by Lemma 2.10 (2).

Since $F_p[V]^{D_{2p}} = F_p[x^2, y^p - y(x^{p-1})]$ and by Proposition 2.5, we see that

$$\sqrt{(\mathrm{Im}(Tr^{D_{2p}}))^e} \bigcap F_p[V]^{D_{2p}} = (x)_{F_p[V]} \bigcap F_p[x^2, y^p - y(x^{p-1})] = (x^2)_{F_p[V]^{D_{2p}}}.$$

Hence $\sqrt{\mathrm{Im}(Tr^{D_{2p}})} \subseteq (x^2)_{F_p[V]^{D_{2p}}}$.

On the other hand, in order to prove $(x^2)_{F_p[V]^{D_{2p}}} \subseteq \sqrt{\mathrm{Im}(Tr^{D_{2p}})}$, it suffices to show that there exists a number k, such that $(x^2)^k \in \mathrm{Im}(Tr^{D_{2p}})$. In fact,

$$\begin{aligned} Tr^{D_{2p}}(y^{p-1}) &= \sum_{g \in D_{2p}} gy^{p-1} = 2\sum_{k=0}^{p-1}(y+kx)^{p-1} \\ &= 2\sum_{k=0}^{p-1}(y^{p-1} + (p-1)y^{p-2}(kx) + \cdots + (p-1)y(kx)^{p-2} + (kx)^{p-1}) \\ &= 2\sum_{k=0}^{p-1} y^{p-1} + 2(p-1)y^{p-2}x\sum_{k=0}^{p-1} k + \cdots + 2(p-1)yx^{p-2}\sum_{k=0}^{p-1} k^{p-2} + 2x^{p-1}\sum_{k=0}^{p-1} k^{p-1}. \end{aligned}$$

By Lemma 2.8, $\sum_{k=1}^{p-1} k^i = 0$, $i = 1, \dots, p-2$, it follows that

$$Tr^{D_{2p}}(y^{p-1}) = 2x^{p-1}\sum_{k=0}^{p-1} k^{p-1} = 2x^{p-1}\sum_{k=1}^{p-1} k^{p-1}.$$

And by Lemma 2.9, $k^{p-1} \equiv 1 \pmod p$, we conclude that

$$\begin{aligned} Tr^{D_{2p}}(y^{p-1}) &= 2x^{p-1}\sum_{k=1}^{p-1} k^{p-1} = 2x^{p-1}\sum_{k=1}^{p-1} 1 \\ &= 2x^{p-1}(p-1) = -2x^{p-1} = -2(x^2)^{\frac{p-1}{2}}. \end{aligned}$$

This implies $(x^2)^{\frac{p-1}{2}} \in \mathrm{Im}(Tr^{D_{2p}})$, and the proof is completed. □

Theorem 2.12 *Let $\varrho : D_{2p} \hookrightarrow GL(2, F_p)$ be a faithful representation of the group D_{2p} over the prime field F_p, afforded by the matrices*

$$\varrho(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \varrho(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $\mathrm{Im}(Tr^{D_{2p}}) = (x^{p-1})_{F_p[V]^{D_{2p}}}$.

Proof By the proof of Theorem 2.11, we see that $Tr^{D_{2p}}(y^{p-1}) = -2x^{p-1}$, so it is obvious that $\mathrm{Im}(Tr^{D_{2p}}) \supseteq (x^{p-1})_{F_p[V]^{D_{2p}}}$. On the other hand, in order to prove $\mathrm{Im}(Tr^{D_{2p}}) \subseteq (x^{p-1})_{F_p[V]^{D_{2p}}}$, we need only consider the image of the monomial $x^r y^s$, $r, s \in N$, since transfer is a linear homomorphism.

$$\begin{aligned} Tr^{D_{2p}}(x^r y^s) &= \sum_{i=0}^{p-1} a^i(x^r y^s) + \sum_{i=0}^{p-1} a^i b(x^r y^s) \\ &= x^r \sum_{i=0}^{p-1} a^i(y^s) + (-1)^r x^r \sum_{i=0}^{p-1} a^i(y^s) \\ &= (1+(-1)^r)x^r \sum_{i=0}^{p-1} a^i(y^s) = (1+(-1)^r)x^r \sum_{i=0}^{p-1} (y+ix)^s \\ &= (1+(-1)^r)x^r (\sum_{i=0}^{p-1} (y^s + sy^{s-1}ix + \cdots + C_s^k y^{s-k}(ix)^k + \cdots + (ix)^s)) \\ &= (1+(-1)^r)x^r (\sum_{i=0}^{p-1} y^s + \sum_{i=0}^{p-1} sy^{s-1}ix + \cdots + \sum_{i=0}^{p-1} C_s^k y^{s-k}(ix)^k + \cdots + \sum_{i=0}^{p-1}(ix)^s) \end{aligned}$$

By Lemma 2.8, we have

(1) When $s < p-1$, then $k \leq p-2$ and all $\sum_{i=0}^{p-1} C_s^k y^{s-k}(ix)^k = 0$, hence $Tr^{D_{2p}}(x^r y^s) = 0$.

(2) When $s \geq p-1$, if $k \leq p-2$, then the terms $\sum_{i=0}^{p-1} C_s^k y^{s-k}(ix)^k = 0$, hence

$$Tr^{D_{2p}}(x^r y^s) = (1+(-1)^r)x^r \Big(\sum_{i=0}^{p-1} C_s^{p-1} y^{s-p+1}(ix)^{p-1} + \cdots + \sum_{i=0}^{p-1}(ix)^s \Big).$$

So we obtain $x^{p-1} | Tr^{D_{2p}}(x^r y^s)$, for all $r,\ s \in N$. Thus, $\mathrm{Im}(Tr^{D_{2p}}) \subseteq (x^{p-1})_{F_p[V]^{D_{2p}}}$, and the theorem is proved. □

Acknowledgements The authors would like to thank the referees for their time and useful comments.

References

[1] M. D. NEUSEL. *Invariant Theory*. Student Mathematical Library, vol.36, Amer. Math. Soc., 2006.

[2] L. SMITH. *Polynomial invariants of finite groups. A survey of recent developments*. Bull. Amer. Math. Soc. (N.S.), 1997, **34**(3): 211–250.

[3] M. D. NEUSEL, L. SMITH. *Invariant Theory of Finite Groups*. American Mathematical Society, Providence, RI, 2002.

[4] G. H. HARDY, E. M. WRIGHT. *An Introduction to the Theory of Numbers*. Fifth Edition, The Clarendon Press, Oxford University Press, New York, 1981.

[5] Jizhu NAN, Ying WANG. *Introduction to Commutative Algebra*. Science Press, Beijing, 2012. (in Chinese)